

DORA ADDENDUM

This EU DORA Addendum (this “**DORA Addendum**”) forms part of the Services Agreement between Sedra and Customer (the “**Agreement**”) and applies only if and to the extent Customer is required to comply with the EU Digital Operational Resilience Act (EU Regulation 2022/2554), together with its delegated acts (“**DORA**”), in connection with its use of the Services. Capitalized terms not defined in this DORA Addendum have the meanings given in the Services Agreement. If there is a conflict between this DORA Addendum and the Agreement, this DORA Addendum will control solely with respect to its subject matter.

1. Scope. This DORA Addendum applies only to the Services used by or for Customer in a manner that is in scope of Customer’s DORA compliance obligations. This DORA Addendum does not apply to any Services, use cases, Affiliates, or activities that are not subject to DORA. Nothing in this DORA Addendum requires Sedra to provide commitments broader than those required under DORA as applicable to the Services.

2. Roles; Customer Assessment. For purposes of this DORA Addendum, Customer is the relevant ‘financial entity’ and Sedra is the relevant ‘ICT third-party service provider’ under DORA. References to Customer also include any Customer Affiliate covered by the Agreement to the extent that Affiliate is required to comply with DORA in connection with its use of the Services.

3. Current Classification. As of the effective date of this DORA Addendum, Sedra is not designated as a ‘critical ICT third-party service provider’ under Article 31 of DORA and does not provide ‘critical or important functions’ as defined in Article 3(22) of DORA. Customer remains solely responsible for its own regulatory assessments, including whether its use of the Services is subject to DORA and whether the Services support a critical or important function for Customer.

4. Location and Nature of Services. Customer acknowledges and agrees that: (a) the Sedra DPA includes a clear and complete description of all ICT services to be provided by Sedra under the Agreement; and (b) Sedra provides services, processes data and/or stores data in the United States and Kuwait. In the event of any material change to these service locations, Sedra will notify Customer in writing at least ten (10) days in advance and provide sufficient information to enable Customer to assess the risks and impact.

5. Regulatory Cooperation. Upon your reasonable request and at your expense, Sedra will timely and diligently cooperate with any competent authority having legal jurisdiction over your financial regulated activities to the extent required by applicable law, provided that all Sedra Confidential Information and the confidential information of other customers shall be fully protected to the fullest extent permitted by applicable law.

6. Data Security.

6.1 Security measures. Sedra has adopted and will maintain administrative, technical, physical, and organizational security measures to protect Customer Data that we Process (including Personal Data) against accidental or unlawful destruction, loss, alteration, disclosure or access, as described in our DPA. Sedra will maintain such security measures to provide a level of protection that is appropriate to the risks concerning confidentiality, integrity, availability and resilience of our systems and the Services, while also

taking into account the state of the art, implementation costs, the nature, scope and purposes of processing, as well as the probability of occurrence and the severity of the risk.

6.2 Incidents. In the event of an ICT-related incident (as defined in DORA) with respect to the Services, Sedra will provide assistance to Customer at no additional cost, or at a cost that is determined by the parties ex-ante, consistent with the incident response procedures for Data Breaches set forth in the DPA.

6.3 Training Programs. No more than once every twelve (12) calendar months, upon at least thirty (30) days prior notice and at your expense and request, we will designate no more than one (1) Sedra employee to participate in security awareness programs or digital operational resilience training related to your information security.

7. Additional Obligations for “Supporting Critical or Important Functions.” The following apply to you only if and solely to the extent you have determined that the Services “supports” a “critical or important function” under DORA.

7.1 Service levels; Notification and Assistance. Customer will be entitled to our standard warranties and services levels as described in the Agreement and our SLA. Sedra will provide reasonable information to Customer of any circumstance that may have a material impact on Sedra’s ability to effectively provide the Services in line with agreed service levels. Sedra may provide this information via email or other electronic means, including by posting security bulletins or maintaining an online status page. You may subscribe to notifications of updates to these resources, and it is your obligation to subscribe to receive notifications and updates.

7.2 Business continuity. Sedra will implement, maintain and routinely test security incident, business continuity and disaster recovery policies, plans and procedures with a view to maximizing availability and minimizing business and service disruptions.

7.3 TLPT Cooperation. Sedra will fully participate and cooperate in Customer threat-led penetration testing (TLPT) programs pursuant to Articles 26 and 27 DORA, provided such testing does not impact or compromise the security, integrity or availability of the Services.

7.4 Customer’s Right to Monitor. Sedra acknowledges and will cooperate with Customer’s right to monitor, on an ongoing basis, Sedra’s performance under the Agreement, which may entail rights of access, inspection, audit, and the right to make on-site copies of relevant documents. Such rights may be exercised by Customer, its competent authority, or an appointed third party. Such rights will be exercised under the conditions for general compliance audits set forth in the Sedra DPA, provided that additional audits may be performed if required by Customer’s competent authority. If a request for access, inspection or audit is denied due to a threat to security or other service environments, Sedra will provide alternative assurances to verify compliance.

7.5 Exit Arrangements. Upon expiration or termination of the Agreement or applicable Order Form, Sedra will provide Customer with reasonable assistance to facilitate transition from the Services, to the extent expressly set out in the Agreement, applicable Order Form, or Documentation. Any additional transition or exit services requested by Customer will be subject to mutual agreement and, unless otherwise agreed, Sedra’s then-current rates.

7.6 Subcontracted Services. Sedra's DPA provisions relating to Subprocessors, including any applicable notice, objection, and termination rights, also apply for purposes of subcontracting under this DORA Addendum. In addition, Sedra will maintain a Subprocessor oversight process reasonably designed to assess the suitability of its Subprocessors in light of the Services they provide, including with respect to security, confidentiality, resilience, and business continuity, as appropriate. Sedra will monitor Subprocessors on an ongoing basis through commercially reasonable means. To the extent required by DORA and applicable to the Services, Sedra will impose contractual obligations on relevant Subprocessors reasonably designed to enable Sedra to meet its applicable obligations under this DORA Addendum. Where direct rights of access, inspection, or audit are not reasonably available from a Subprocessor, Sedra may satisfy the relevant requirement through alternative means, such as independent audit reports, certifications, summaries, or other information reasonably sufficient to demonstrate the Subprocessor's compliance with applicable requirements.

8. Additional Termination Rights. In addition to the other termination rights in the Agreement, Customer may also terminate the Agreement immediately upon written notice if: it is necessary to comply with applicable law, including any of the circumstances set out in Article 28(7) of DORA; directed by a competent authority of Customer; or Customer's regulator can no longer effectively supervise Customer as a result of the terms of, or circumstances related to, the Services or the Agreement. In the event of the expiration or termination of the Agreement, including in the event of insolvency, resolution, or discontinuation of the business operations of Sedra, all Personal Data and other Customer information processed by Sedra in connection with providing the Services to Customer will be accessible and recoverable by Customer and returned to Customer in an easily accessible format, in accordance with the existing procedures set forth in the Agreement (as applicable to you) and DPA.

9. Indemnification. Section 12.2 of the Agreement is amended to hereby add the following as an additional Customer indemnity: "(d) Customer's financial regulatory compliance obligations under the EU Digital Operational Resilience Act (EU Regulation 2022/2554), the UK Financial Services and Markets Act 2023, or similar legislation."

10. Updates. Sedra may update this DORA Addendum from time to time on a prospective basis to address legal, security, operational, or technical developments. Any material changes will be handled in accordance with the Agreement. If changes in DORA or its delegated acts materially affect the parties' obligations under this DORA Addendum, the parties will discuss in good faith any amendments reasonably necessary to address such changes. Nothing in this section obligates Sedra to agree to terms that materially expand its obligations beyond those required by applicable law or inconsistent with its generally offered Services.